I✶I Communications Security Establishment Canada   Centre de la sécurité des télécommunications Canada

JAN 1 2 2017

BRIEFING NOTE FOR CHIEF, CSE

Continuous/Technically Assisted Audit: Memberships

(For Review and Approval)

Summary

- In December 2016, the Departmental Audit Committee (DAC) accepted DGAEE's *Continuous/Technically Assisted Audit: Memberships*

- DGAEE requests that the Chief, CSE approve this report to both finalize the audit and to enable the audit team to include the recommendations and ensuing action plan in the Management Action Plan Progress Report

- DGAEE also requests approval from the Chief, CSE to publish the audit report on the DGAEE internal website

Background

The audit findings from the *Continuous/Technically Assisted Audit: Memberships* were presented to the DAC in December 2016. The following findings were tabled:

- Exercise of financial authority for the remittance of memberships was carried out by persons with appropriate delegated financial authority and with an appropriate segregation of duties.

- Individual membership fees were remitted in accordance with policy and directive requirements, or had documented rationale for exceptional approval from DG HR.

- The process to obtain corporate memberships differed from the process outlined in CSE's *Directive on Membership, Registration and Licensing Fees* (HRH-65).

- Tracking of individual and corporate memberships was incomplete and did not have a reconciliation process with FAMIS.

The management action plans provided by the relevant stakeholders were deemed satisfactory by the DAC.

Canada

At the conclusion of the presentation, the DAC recommended the audit for Chief, CSE approval.

Decision/Direction

It is recommended that the Chief, CSE approve the *Continuous/Technically Assisted Audit: Memberships* and permit the document's publication to the DGAEE internal website.

Next Steps

Once approval has been received, the report will be finalized, translated, and published. In addition, the Management Action Plan Progress Report will be updated to reflect the audit's recommendations and Management Action Plan.

[signature]

Joanne Renaud, CPA, CMA & Certified Coach
Director General, Audit, Evaluation and Ethics

Approved/Not Approved

[signature]

Greta Bossenmaier, Chief

Communications Security   Centre de la sécurité
Establishment   des télécommunications

Continuous / Technically Assisted Audit: Memberships

Final Report

Directorate of Audit, Evaluation and Ethics

January, 2017

CERRID #30964386

Canada

Conformance and Assurance Statement

Continuous / technically assisted (CTA) auditing refers to the proactive monitoring of key, risk-based practices and controls using technology and audit trade skills as an efficient and effective mechanism to support results achievement and management's active monitoring efforts. It presents a unique value proposition for Internal Audit as it can identify, in a timely manner and with minimal resources, anomalies resulting from the intelligent interrogation of databases that may warrant explanation or investigation.

Performing CTA audit testing on a periodic basis provides:

- Reasonable assurance that controls are operating as intended and that the associated risks are being mitigated adequately;

- Detection of anomalies that might indicate errors or fraud; and

- Tracking and escalation of exceptions for possible action.

Although not as high as if resulting from a full audit, the level of assurance that results from this audit should be useful to management.

To the extent considered appropriate and applicable, the Institute of Internal Auditors standards were applied in the conduct of this engagement.

Engagement and Report History

Audit Phases	Reviewer	Changes	End Date
Planning	DGAEE		July 2016
Examination	DGAEE		September 2016
Office Draft	DGAEE		September 2016
Clearance and Discussion Draft	DGAEE		October 2016
Final Report	DAC		December 2016
Final Approval	Chief		January 2017

For information about this report, contact the Director General, Audit, Evaluation and Ethics (DGAEE).

Table of Contents

Introduction

Parliament and Canadians expect the federal government to manage public funds with the highest standards of fiscal prudence, accountability and transparency. While fundamental governance principles apply to government expenditures at all levels, it is understood that specific membership-related expenditures are necessary in order for departments to effectively deliver services to Canadians.

1.1 Background

Membership expenditures at CSE were most recently examined in the 2011 *Audit of Memberships*. The audit assessed the extent to which membership fee payments were compliant with applicable authoritative documents, and the adequacy of the management control framework that administered payments. The audit produced four recommendations, all of which have completed management action plans.

1.2 Audit Objective, Scope and Limitations

As a follow-up of the effectiveness of the controls that were enhanced as a result of the 2011 audit, DGAEE conducted the *Continuous / Technically Assisted Audit: Memberships*. This audit was performed pursuant to the *CSE Audit and Evaluation Plan for FY 2016-17 to FY 2020-21*[1] that was approved by the Chief, CSE on 7 July 2016.

The engagement's objective was to provide reasonable assurance to management that individual and corporate membership expenditure were remitted for valid expenses in compliance with authorized policies. The scope of the audit was individual and corporate membership transactions for fiscal year (FY) 2015-16.

Memberships that may have been included in the cost of a training course or conference registration are not examined in this audit. Such memberships offer reduced registration costs to attendees though employees are prohibited from accepting these offers unless the membership is previously approved. These memberships are out of the scope of this audit as examination would require analyzing all conference travel claims from FY 2015-16.

Methodology

The audit examined a sample size of 111 potential membership transactions. Analysis of the 111 transactions found 56 were related to individual memberships, 6 were related to corporate memberships and 49 were out of scope.[2] The following data collection methodologies were employed to develop findings and conclusions.

---

[1] Refer to CERRID #29757242.
[2] See Annex A for additional information on determination of sample size.

Tests: Tests for this audit examined control processes related to the 1) administration, 2) remittance and 3) tracking of membership expenditures to ensure accordance with applicable policies and directives:

1) Exercise of financial authority is carried out by persons with the appropriate delegated authority and a segregation of duties exists to reduce the possibility of erroneous or inappropriate action;

2) Remitted membership fees are in accordance with policy and directive requirements; and

3) Remitted membership fees are tracked and recorded with effective quality control measures for audit purposes.

Document Review: Records from Labour Relations, Information Discovery (CIO-E   formerly Library Information Services) and Finance were obtained and used as the basis of the evidence for this audit. The following relevant CSE and government policies and directives were reviewed:

- *Assistance for Spouses or Common-Law Partners* (FSD 17);[3]

- *Corporate Memberships and Library Information Services (LIS) Role*;

- *CSEC Delegation of Authorities for Financial Administration* (FIN-01-01);

- *Directive on Membership, Registration and Licensing Fees* (HRH-65);

- *Financial Officer to Chief Financial Officer Career Path*;[3]

- *Financial Administration Act*;

- *Membership Fees Provisions of Collective Agreement*;

- *Policy on Counselling and Advisory Program* (HRH-81);[3]

- *Policy on Psychological Assessment Services* (HRH-18);[3]

- *Polygraph Testing Policy* (SEC-201);[3] and

- *Rescission of Membership Fees Policy*.

Interviews: Interviews and email correspondence were conducted with Labour Relations Advisors, Information Discovery Supervisor and Advisors, Finance Accounting Operations Manager, Supervisor and Staff, and Human Resources Analytics Advisors (HR).

Findings

This section summarizes the main findings of the three tests conducted to ensure that the expected controls were working as expected.

---

[3] These documents were examined during the process of looking at rationale behind membership claims.

3.1 Administration Control

Audit Test*: Exercise of financial authority is carried out by persons with the appropriate delegated authority and a segregation of duties exists to reduce the possibility of erroneous or inappropriate action.*

The purpose of this test was to verify that the Financial Administration Act Section 34 certification authority for each of the 56 individual membership transactions and 6 corporate memberships held the appropriate financial signing authority, and that, as per section 3.8 of CSE's *Delegation of Authorities for Financial Administration* (FIN-01-01), a segregation of duties existed between the certification authority and the person benefitting from the claim.

To assess compliance with delegated authorities, electronic and/or hard copies of individual and corporate membership claims were examined against the CSE Financial Signature Card Application to verify that the persons signing had the designated Section 34 authority for the Responsibility Centre (RC). Claims were also reviewed to ensure a segregation of duties.

Table 1 – Section 34 & Segregation of Duties Test

Test	Compliance
Appropriate Section 34 authority	100%
Segregation of duties	100%

Individual Memberships

Fifty-five of the 56 individual membership transactions were examined to verify appropriate Section 34 authority and segregation of duties. The hard copy for one claim could not be found. The examination found 100% compliance for the 55 claims assessed.

Verification of Section 34 authority could be strengthened by the signing authority printing his or her name and including the date of signing. The printed name field was left blank on 8 out of 55 GACs and only just over half Section 34 authorities (29 out of 55) included the signing date. Though the signature block does not specifically request a signing date, it assists auditing to verify proper signing authority was held at the date of the signing.

Corporate Memberships

Six corporate memberships were examined to verify appropriate Section 34 authority. The examination found 100% compliance for the 6 claims assessed. Segregation of duties was not examined for these memberships as they were corporate memberships that were not benefiting an individual.

3.2 Remittance Control

Audit test*: Remitted membership fees are in accordance with policy and directive requirements.*

CTA Audit – Memberships   CONFIDENTIAL

The purpose of this test was to verify that remitted fees for individual and corporate memberships examined were done in accordance with CSE policy and directive requirements.

Individual Memberships

Remitted individual memberships were examined to verify that the membership was recorded in the Labour Relations master list, and to confirm that the membership was either a federal requirement for the employee to carry out the functions of his or her position or in direct support of a government program, as per section 6.9.1 FIN-01-01.[4]

The audit found that 52 of the 56 individual membership transactions met the criteria of being a requirement of the individual to carry out duties of the position or in support of a government program. Three memberships that did not meet the required criteria for reimbursement were granted exceptional approval from DG HR. Documentation for the remaining membership could not be found in Labour Relations, Finance or Information Holding Services records and thus could not be examined for rationale of its remittance.

The 56 membership transactions examined were held by 48 different individuals, with some persons holding more than one membership. Data provided by HR showed that 44 of the 48 individuals remained for the duration of the FY in the position for which the membership was either a requirement for the claimant to carry out the functions of his or her position or in support of a government program. Of the remaining four people that had changed positions since claiming the membership, three individuals had been promoted within the same directorate into positions that also required the membership, and one individual moved to a new group near the end of FY 2015-16.

Of note, some   practitioners were remitted for multiple provincial or national professional association memberships. According to HRH-81, practitioner positions require registration with "a professional association," indicating that only one such registration is required to carry out duties of the position. While each remitted membership on its own met the criteria of being a requirement of the position, Labour Relations has confirmed that starting in FY 2017-18 only one professional association membership will be remitted for   practitioners.

Corporate Memberships

Six corporate memberships for FY 2015-16 were examined to verify that the requests followed the process of CSE's *Directive on Membership, Registration and Licensing Fees* (HRH-65). This directive's process calls for the RC manager requesting the corporate membership to consult with Information Discovery (formerly Library Information Services) to ensure the membership was not already held at CSE. If it was not, the manager commits the funds in the Financial and Asset Management Information System (FAMIS) and forwards an approved Corporate

---

[4] See Annex B for Individual Membership Remittance Process with Internal Control Systems.

Membership Form to Information Discovery, who will pay the fees and charge the cost to the FAMIS commitment, and record the membership in a master list.

The audit found that none of the corporate memberships followed the full process of HRH-65. Table 2 compares HRH-65 to Information Discovery's internal document on corporate membership guidelines and to the corporate membership practice of Information Discovery in FY 2015-16.

Table 2 – Comparison of Procurement of Corporate Memberships

HRH-65 – CSE Directive on Membership, Registration and Licensing Fees	Information Discovery Corporate Membership Guidelines	Audit Findings for FY 2015-16 Corporate Memberships
Prior to approving a corporate membership, the RC manager should consult with Information Discovery to ensure the membership has not already been obtained.	Information Discovery will not determine the merit of the membership. RC managers are responsible for including justification for the membership with the membership request for documentation purposes.	Clients consulted with Information Discovery prior to purchase for four of six memberships. One membership was automatically renewed by Information Discovery based on past years' consultation. One membership was procured by client without consultation.
RC manager submits approved Corporate Membership Application Form to Information Discovery.	Client submits a Corporate Membership Application Form or written request which includes justification and funding commitment to Information Discovery.	Clients submitted an application for three memberships and provided justification for two other memberships.
RC manager ensures that a commitment for costs is created in FAMIS.	RC manager is required to provide the funds for the membership.	Information Discovery does not require financial coding; they provide permission for the RC managers to purchase.
Information Discovery will pay the fees and charge the costs to the appropriate RC manager's budget / commitment.	Once the application form or request has been received, Information Discovery will procure access to the membership on behalf of CSE.	RC managers paid for and procured five memberships. One membership renewal was paid for and procured by Information Discovery.
Information Discovery has the role of ensuring that a monitoring system is established for all corporate memberships.		Corporate memberships are recorded but not monitored.
Information Discovery maintains the corporate membership master list for each fiscal year.	Information Discovery maintains the corporate membership master list for each fiscal year.	Information Discovery maintains the corporate membership master list for each fiscal year.

Recommendation (Moderate)

1) It is recommended that Director, Information Management (CIO-E) ensures that the Information Discovery's approval and procurement process for corporate memberships aligns with the Directive on Membership, Registration and Licensing Fees (HRH-65).

3.3 Tracking Control

Audit test: *Remitted membership fees are tracked and recorded with effective quality control measures for audit purposes.*

The purpose of this test was to verify that remitted individual and corporate membership fees were tracked and recorded with effective quality control measures for audit purposes.

CTA Audit – Memberships   CONFIDENTIAL

According to section 6.1 of HRH-65, CSE is required to record membership and registration fees and retain information on the total amount spent on memberships and the number of memberships held for each fiscal year. This reporting requirement is also outlined in section 6.9.3 of FIN-01-01.

Section 4.3 of HRH-65 assigns to Labour Relations the responsibility of reviewing, monitoring and recording individual membership fees forwarded by RC managers. Labour Relations' FY 2015-16 membership master list identified 55 approved memberships, of which 51 of these were claimed and remitted. As Labour Relations does not track whether a membership was remitted, there was no notation in the master list of the 4 memberships listed but not claimed.

FAMIS queries identified 5 remitted memberships that were not in Labour Relations' master list. This included 1 membership for which no documentation could be obtained for this audit.[5]

The total CSE expenditure validated in FAMIS for all individual memberships totalled
for FY 2015-16. This differed slightly from the Labour Relations master list total of
The difference between the two amounts is due to the following:

- Labour Relations records the amount with tax included while FAMIS transactions deduct tax from Canadian purchases;

- Approximately   of non-membership related costs were incorrectly coded to General Ledger (GL)   Professional Membership Fees as part of a GAC that included membership fees;

- Unless a request for approval contains a GAC with the amount paid in Canadian dollars, fees in US dollars are not converted into Canadian dollars in the master list; and

- Five remitted memberships were not listed in the Labour Relations master list.

In section 5.2 of HRH-65 the responsibility for maintaining a master list of corporate memberships is assigned to Information Discovery. The corporate membership master list for FY 2015-16 identified two memberships. An additional three corporate memberships were approved by Information Discovery but were not recorded in the master list. Finally, one membership was procured without Information Discovery consultation.

The total amount of all corporate memberships in FAMIS was   The Information Discovery master list recorded the cost of the two tracked memberships in the original currency (one membership was in US dollars).

The audit also examined the use of financial coding to determine if memberships were coded to the correct GL and if sub-project codes were used for tracking purposes. Evidence demonstrated that the majority of individual and corporate memberships (97% or 64 out of 66)

---

[5] This membership claim for   was identified through GL coding and purchase description in FAMIS.

were correctly coded to the Professional Membership Fees GL   Given that there were only 68 transactions[6] in FAMIS for FY 2015-16 that were coded to GL   it is the audit's opinion that there would be little benefit to the introduction of sub-project codes specific to memberships.

Recommendation (Minor)

2) It is recommended that Director, Information Management (CIO-E) establish a process for periodic reconciliation between Information Discovery's master list of corporate memberships and corporate membership expenditures in FAMIS.

Recommendation (Minor)

3) It is recommended that DG HR establish a process for periodic reconciliation between Labour Relation's approved master list of individual memberships and individual membership expenditures in FAMIS.

Conclusion

Based on the tests performed, the audit found:

1) Strong administrative controls and appropriate segregation of duties around the exercise of financial authority for individual memberships.

2) In most cases, remittance controls for individual memberships were in accordance with policy and directive requirements, and the noted example of positions remitted for registration with multiple professional associations will be addressed by Labour Relations to correct for FY 2017-18. Evidence of the remittance process for corporate memberships found inconsistency between Information Discovery's membership approval and procurement process and the process outlined in HRH-65.

3) Tracking and recording controls were stronger for individual memberships than for corporate memberships, the latter of which recorded only two of six memberships for FY 2015-16 in the master list. Both master lists did not track and reconcile with FAMIS the total amount spent in FY 2015-16. GL codes are almost always used appropriately for membership claims and the small number of claims coded to the memberships GL indicates that there is no need for usage of sub-project codes to help monitor and track membership expenditures.

---

[6] The 68 transactions represented   of CSE transactions, and   of CSE's total expenditure in FY 2015-16.

Audit Recommendations and Management Action Plan

#	Observation	Recommendation	Management Action Plan	OPI	Target Date
Audit Ranking: [7] **Moderate**					
1	The audit found that none of the six corporate memberships obtained for CSE followed the full process of the *Directive on Membership, Registration and Licensing Fees* (HRH-65).	It is recommended that Director, Information Management (CIO-E) ensures that the Information Discovery's approval and procurement process for corporate memberships aligns with the *Directive on Membership, Registration and Licensing Fees* (HRH-65).	Annual communiqué on Corporate memberships to CSE explaining process and authority for managing memberships. Hold meeting with CIO-E library staff to share results of audit and go through the revised corporate membership guidelines in alignment with HRH-65 to ensure that all staff are aware of procurement procedures, definitions and proper saving of corporate membership documentation.	CIO-E	March 2017
Audit Ranking: Minor					
2	The audit found that Information Discovery's master list of corporate memberships was incomplete, with only two of six memberships recorded.	It is recommended that Director, Information Management (CIO-E) establish a process for periodic reconciliation between Information Discovery's master list of corporate memberships and corporate membership expenditures in FAMIS.	Create reconciliation process and add to CIO-E corporate membership guidelines. Ensure reconciliation between FAMIS and CIO-E list is done quarterly.	CIO-E	March 2017
Audit Ranking: Minor					
3	The audit found that Labour Relations' master list of individual memberships was incomplete, and did not match the memberships processed in FAMIS.	It is recommended that DG HR establish a process for periodic reconciliation between Labour Relation's approved master list of individual memberships and individual membership expenditures in FAMIS.	At the end of each fiscal year Finance will provide Labour Relations with a list of all membership payments processed for that fiscal year. Labour Relations will reconcile the list of membership payments from Finance against the Labour Relations membership list.	Director HR Programs Director Finance Operations	March 2017

[7] See Annex C for descriptions of audit recommendation rankings.

Annex A – Audit Sample

The audit sample was determined first by examination of the FY 2015-16 membership master lists of Labour Relations and Information Discovery. A total of 57 memberships were identified, with 55 individual memberships from Labour Relations' master list and 2 corporate memberships from Information Discovery's master list.

CSE's FAMIS financial system was cross-referenced to verify remittance amounts and to identify potential membership costs that were not identified in the master lists. This search identified 54 additional transactions for examination, bringing the total to 111 transactions. The 54 additional transactions were discovered through these FAMIS queries:

- All financial line items under GL   Professional Membership Fees;

- All financial line items with "Memb" in the description field;

- All financial line items coded to GLs   Professional Services,   Training Inside Canada,   Training Outside Canada, and   Education, Tuition, Exam;[8] and

- All financial line items with "Toast",   in the description field.[9]

Table 3 shows all 111 transactions identified and whether they were determined to be in or out of scope for this audit.

Table 3 – Transactions Examined

	Transactions Examined	#	Total
In Scope	Individual Memberships in Labour Relations Master List and FAMIS	51	62
	Individual Memberships in FAMIS Only	5	
	Corporate Memberships in Information Discovery Master List and FAMIS	2	
	Corporate Memberships in FAMIS Only	4	
Out of Scope	Individual Memberships in Labour Relations Master List Only*	4	49
	Financial Coding Transactions	8	
	ToastMasters Training**	27	
	Other Transactions Deemed Out of Scope***	10	

These memberships were not claimed and therefore are not included in the individual membership total

**ToastMasters transactions often were described as memberships in their FAMIS descriptions but are financially coded and treated as an in-house learning activity.*

****These items included subscriptions, Foreign Service Directive payments, and professional fees.*

---

[8] These GLs were searched based on results following the "Memb" FAMIS search.
[9] These phrases were searched following results from the "Memb" and GL searches. "Toast" refers to ToastMasters memberships and   items.

CTA Audit – Memberships   CONFIDENTIAL

Electronic and/or hard copies of the 111 individual and corporate membership transactions were obtained from Finances Accounting Operations. The 56 individual and 6 corporate membership claims examined in this audit are listed in Table 4 and Table 5, respectively. Exceptional approval for   and the   was granted by DG HR. Exceptional approval was also granted for

who were on a developmental path towards

Table 4 – Individual Membership Transactions by Organization

Memberships by Organization	#	Requirement of Position	In Support of a Program	Exceptional Approval
				✓
		✓		
		✓		
				✓
		✓		✓
		✓		
		✓		
			✓	
			✓	
		✓		
		✓		

* some staff in DGAEE also hold   memberships which are paid for by Treasury Board Secretariat
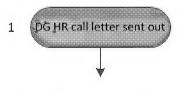
** indicates a membership that could not be verified

Table 5 – Corporate Memberships Process Comparison

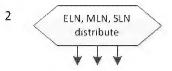| Memberships by Organization	Corporate Application Form Submitted	Approved by Information Discovery	Membership Procured by
	✓	✓	Client
		✓	Client
		✓	Client
			Client
		✓	Information Discovery
	✓	✓	Client

Annex B – Individual Membership Remittance Process with Internal Control Systems
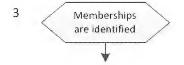
This process chart represents a description of the individual membership remittance process with internal control systems, which are identified in purple boxes.

1 — DG HR call letter sent out

A call for individual memberships goes out in the first quarter of the fiscal year from DG HR to the Executive Leadership Network (ELN), Manager Leadership Network (MLN) and Supervisor Leadership Network (SLN) email distribution lists.

2 — ELN, MLN, SLN distribute
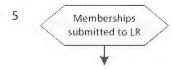
ELN, MLN and SLN distribute amongst staff.

3 — Memberships are identified

Individual membership claims are identified.

4 — Control – DG Review

Completed individual membership forms are reviewed and approved at the applicant's DG level.

5 — Memberships submitted to LR

Approved forms are submitted to Labour Relations.

6 — Recorded in LR Master List

Labour Relations records the request in the membership master list.

7 — Control – LR Review

Labour Relations reviews to ensure the membership meets the requirement as necessary for an individual to carry out duties of position, or that the membership is in support of a government program. Exceptional approval may be sought at this control level if the membership has justification.

   a. If the membership is a requirement for the individual to carry out duties of the position or is in support of a government program, Labour Relations prepares a briefing note for DG HR approval.

8 — Briefing note to DG HR / DCCS prepared

   b. If there is a business case for the membership to be granted, Labour Relations prepares an exceptional approval

email request for DG HR or DCCS.

9	Control – DG HR Review	Membership requests and briefing notes are sent to DG HR for approval.
10	Memberships sent to Finance	Following DG HR approval, membership requests are forwarded to Finance. In cases where the membership has not already been paid, DG HR approval is sent to the claimant, who upon purchase of the membership forwards the completed GAC and confirmation of DG HR approval to Finance.[10]
11	Control – Finance Review	Finance reviews membership claims to verify receipts are included and financial signing authorities are correct. If signing authority is missing, the claim is returned by internal mail to the claimant for proper approval. If claim is missing receipts or other information, Finance will contact the claimant.
12	Membership Remitted	If claim is has proper receipts and signing authority, payment is processed and the membership is remitted.

---

[10] The audit found that because GAC signing sometimes occurs after Labour Relations review, there are instances when Labour Relations cannot confirm the RC paying the claim and thus verify that the membership is a requirement of the individual to carry out the duties of his or her position.

Annex C – Description of Audit Recommendation Ranking

- **Major**: A key control does not exist, is poorly designed or is not operating as intended. Corrective action is required as soon as possible to avoid a potentially significant negative impact involving loss of assets, reputation, resources (including information), or ability to comply with important laws, policies, or procedures.

- **Moderate**: A key control does not exist, is poorly designed or is not operating as intended and the financial and/or reputation risk to the organization is more than inconsequential. However, a compensating control exists. Timely corrective action will avoid a sole reliance on compensating controls and avoid a potentially negative impact involving loss of assets, reputation, resources (including information), or ability to comply with important laws, policies, or procedures.

- **Minor**: A weakness in the design and/or operation of a non-key control. No urgency diagnosed (e.g. best practices). Corrective actions usually contribute to efficiency. These issues may be addressed using management letters.

Annex D – List of Acronyms

CAP	Counselling and Advisory Program
CTA	Continuous / Technically Assisted
DGAEE	Director General Audit, Evaluation and Ethics
DG HR	Director General, Human Resources
FAMIS	Financial and Asset Management Information System
FY	Fiscal Year
GAC	General Allowance Claim
GL	General Ledger
HR	Human Resources
RC	Responsibility Centre

Communications Security
Establishment

Centre de la sécurité
des télécommunications

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

Our file Notre référence
CERRID # 32847528

JAN 1 9 2017

Dear Mr. Calkins:

Thank you for your December 13, 2016 letter regarding the study of the *Security of Canada Information Sharing Act* (SCISA) by the Standing Committee on Access to Information, Privacy and Ethics.

CSE is one of Canada's key security and intelligence organizations. CSE's mandate and authorities are defined in the *National Defence Act* (NDA), which requires CSE to do three things: 1) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities; 2) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and 3) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

As you highlighted in your letter, SCISA lists CSE as an entity that can receive information from another Government of Canada institution. SCISA does not supersede or expand CSE's authorities to collect or receive information from our domestic partners. To date, CSE has not received or disclosed information under SCISA. CSE relies on authorities under the NDA and the provisions of the *Privacy Act*, as well as information sharing arrangements with our domestic security and intelligence partners, when sharing information.
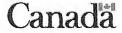
To ensure that information is collected in accordance with its statutory obligations, CSE has policies and systems in place to allow for the validation, tracking and auditing of information received. Such information exchanges involve specific guidelines to ensure that the information is relevant to CSE-mandated activities, and provided to appropriate personnel. Disclosing institutions are encouraged to contact CSE before disclosing any information in order to ensure that CSE's mandate allows for the lawful collection of the information. The implemented process further leverages existing information sharing mechanisms to ensure that information disclosed to CSE is appropriately tracked.

More widely, I would like to highlight that CSE has a responsibility to protect privacy, and we take that responsibility very seriously. Protecting Canadian privacy is a fundamental part of our organizational culture and is embedded within our operational structures, policies and processes. CSE's strong privacy framework includes detailed operational policies, with specific retention periods, and regular training and testing of staff on privacy and compliance knowledge, as well as internal review and independent external review by the Office of the CSE Commissioner. These measures contribute to ensuring that CSE's activities are conducted in a way that protects Canadian privacy interests.

Sincerely,

Greta Bossenmaier
Chief

Canada

Communications Security
Establishment

Centre de la sécurité
des télécommunications

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

JAN 1 9 2017

Our file Notre référence
CERRID # 32847528

M. Calkins,

Je vous remercie pour la lettre que vous nous avez transmise le 13 décembre 2016 concernant l'étude de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique.

Le CST est l'un des principaux organismes de sécurité et de renseignement du Canada. Son mandat et ses pouvoirs sont définis dans la *Loi sur la défense nationale* (LDN), qui confère au CST les trois rôles suivants : 1) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada (GC) en matière de renseignement; 2) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le GC; et 3) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

Comme vous l'avez souligné dans votre lettre, la *Loi sur la communication d'information ayant trait à la sécurité du Canada* définit le CST comme une entité pouvant recevoir de l'information d'une autre institution du GC. La *Loi sur la communication d'information ayant trait à la sécurité du Canada* ne remplace ni n'accroît les pouvoirs du CST en ce qui a trait à la collecte et à la réception de l'information provenant de partenaires nationaux du CST. Jusqu'à maintenant, le CST n'a reçu ni divulgué aucune information en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*. Dans le cadre d'échanges d'information, le CST s'appuie sur les pouvoirs qu'il détient en vertu de la *LDN*, sur les dispositions de la *Loi sur la protection des renseignements personnels* et sur les ententes d'échange d'information conclues avec ses partenaires nationaux de sécurité et de renseignement.

Pour s'assurer que l'information est recueillie conformément à ses obligations statutaires, le CST met en place des politiques et des systèmes visant à valider et à vérifier l'information reçue, et à en faire le suivi. Ces échanges d'information doivent être conformes à certaines directives qui visent à s'assurer que l'information recueillie est pertinente pour les activités du CST et que les bons destinataires la reçoivent. Nous invitons les institutions qui veulent transmettre de l'information au CST à communiquer avec lui avant toute divulgation pour qu'il s'assure que son mandat lui permet de recueillir l'information en toute légalité. Le processus en place comprend d'autres mécanismes d'échange d'information pour veiller au suivi adéquat de l'information transmise au CST.

J'aimerais également souligner de façon générale qu'il incombe au CST de protéger la vie privée des Canadiens et que l'organisme prend cette responsabilité très au sérieux. La protection de la vie privée des Canadiens est un élément fondamental de la culture organisationnelle du CST et fait partie intégrante des structures, des politiques et des processus organisationnels du CST. Le cadre de protection de la vie privée du CST est très rigoureux. Il comporte des politiques opérationnelles détaillées, dont des périodes de conservation précises, des exigences de formation et d'examens réguliers sur la conformité et la protection de la vie privée pour le personnel, ainsi que des examens internes et externes indépendants menés par le Bureau du commissaire du CST. Grâce à ces mesures, on s'assure que le CST effectue ses activités tout en protégeant la vie privée des Canadiens.

Cordialement,

Greta Bossenmaier
Chef

Canada

STANDING COMMITTEE ON ACCESS TO
INFORMATION, PRIVACY AND ETHICS

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

COMITE PERMANENT DE L'ACCES A
L'INFORMATION, DE LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS ET DE L'ETHIQUE

[PAR COURRIEL]

2016-12-13

Greta Bossenmaier, chef
Centre de la sécurité des télécommunications
C.P. 9703, Terminus
Ottawa, Ontario
K1G 3Z4

Madame Bossenmaier,

Dans le cadre de son étude concernant la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique souhaite obtenir des précisions quant au mandat de votre organisation et son rôle en vertu de la *Loi*.

Comme vous le savez, votre organisme fait partie des institutions fédérales destinataires selon l'annexe 3 de la *Loi*.

Plus précisément, le Comité voudrait savoir dans quelle mesure le mandat de votre organisation est lié à la sécurité nationale, et comment votre organisme entrevoit ses responsabilités en vertu de la *Loi* en tant qu'institution destinataire quant à la collecte, la conservation et la communication de renseignements personnels.

Nous vous serions très reconnaissants de transmettre au Comité l'information demandée au plus tard le vendredi 20 janvier 2017, afin que le Comité puisse en prendre compte lors de la reprise de ses travaux à la fin janvier. Au besoin, un représentant de votre organisation pourrait être invité à témoigner devant le Comité pour discuter plus amplement de ce sujet.

Sincères salutations,

Blaine Calkins, député
président

A-2017-00030--00022

STANDING COMMITTEE ON ACCESS TO
INFORMATION, PRIVACY AND ETHICS

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

COMITE PERMANENT DE L'ACCES A
L'INFORMATION, DE LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS ET DE L'ETHIQUE

[BY EMAIL]

2016-12-13

Greta Bossenmaier, Chief
Communications Security Establishment
C.P. 9703, Terminus
Ottawa, Ontario
K1G 3Z4

Dear Ms. Bossenmaier,

In the context of its study of the *Security of Canada Information Sharing Act* (SCISA), the Standing Committee on Access to Information, Privacy and Ethics is seeking clarification on your organization's mandate and its role with regards to the Act.

As you know, you are listed as a recipient institution as per Schedule 3 of the Act.

More precisely, the Committee wishes to know how your organization's mandate relates to national security, and how your organization views its responsibilities under the Act as a recipient institution, with respect to the collection, retention, and further disclosure of personal information.

The Committee would appreciate receiving this information by Friday, January 20, 2017, so that it can consider your response when it resumes sitting in late January. A representative of your organization may be invited to appear before the Committee to discuss the subject matter further, if required.

Best regards,

Blaine Calkins, MP
Chair

A-2017-00030--00023

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

January 27, 2017

MEMORANDUM FOR CHIEF CSE

CSE IM Strategy: Goals for 2017 and Beyond

(For Approval)

Summary

- A CSE Information Management (IM) Strategy was signed in 2012 by the CSE Information Management Senior Official (IMSO), as required by Central Agency at the time. The 2012/13 strategy referenced a five year plan that carried the organization through to FY 2016/17.

- A new CSE IM Strategy has been drafted for FY 2017/18-2019/20, *Enterprise IM Strategy 2017 and Beyond.* This strategy seeks to reinvent, modernize and innovate how the organization manages its information assets. (Reference document: IM Strategy 2016 - 2020.)

- Approval of this strategy by the Chief, CSE is being sought. Government departments are now mandated by Central Agency to have a Deputy-Head approved IM Plan.

- The new IM Strategy was presented to, and endorsed by, the CSE IM/IT Steering Committee on 17 October 2016.

Background

- Treasury Board expectation is that departments will have a Deputy-Head approved IM Plan to demonstrate that IM is integrated as part of organizational business planning and complies with GC horizontal priorities. This requirement is regularly assessed in the Management Accountability Framework (MAF) for IM/IT Stewardship.

- Since the current CSE IM Strategy signed in 2012/13 only carries the organization through to FY 2016/17, a new IM Strategy has been drafted. This strategy sets out

Canada

four areas of opportunity which align with CSE overall strategic direction as well as Central Agency priorities[1]. Moreover, the strategy incorporates feedback from focus group discussions with CSE employees as well as the results of an environmental scan of emerging trends for addressing growing IM challenges across industry and government.

- We have identified four key areas of opportunity that will move CSE along the maturity curve from proactive to transformational IM. The four areas of opportunity are as follows:

    1. **Mature records & Collections Management** – This involves managing the physical and digital records of the department, identifying possible datasets for release through the Government of Canada's Open Government initiative and ensuring adherence to legislative, Treasury Board and Library and Archives Canada requirements for organizational recordkeeping.
    2. **Information Management Compliance** – Establishing a compliance monitoring program to hold the organization accountable for its IM practices is essential to maturing best practices and establishing pro-active measures to address IM accountabilities. A compliance program would reduce our exposure to risk and help the organization meet its legal obligations under the *Access to Information Act* and the *Privacy Act as well as the policy on Management of Government Information.*
    3. **Best-In-Class Service Delivery** – Growing and modernizing IM services and better alignment with mission needs was a theme that resonated with focus groups and was proven through a number of pilots conducted with the mission in 2016/17. CSE's IM Advisory Services has resources with over 10 years of experience with enterprise document and records management systems who could play a leadership role in our growing need shared services and shared information in a TS environment; the Library offers a traditional media monitoring service

    4. **Innovation through Partnership** – This involves experimenting with new ideas like information valuation; engaging partners on challenging projects like building a CSE-wide taxonomy, and finding synergies and economies by sharing knowledge, expertise and products related to open source information discovery.

s.15(1) - DEF

---

[1] The GC's horizontal priorities are set out in the Treasury Board GC Enterprise IM Strategy and revised Treasury Board IM policy suite. Central agency is currently reviewing the GC IM vision and strategy with a view to modernizing IM in government. It has four main goals: improving service to Canadians, enabling workforce flexibility & mobility, bringing government closer to citizens and business and supporting innovation and collaboration. At the same time that Central Agency is updating the GC IM vision and strategy, it is also revising the entire IM policy suite. This revision is moving the focus away from basic recordkeeping to treating information as a strategic asset.

- Each area of opportunity includes a number of strategic goals that serve to address business drivers and describe our desired future state. These goals are supported by key activities that identify the specific steps needed to satisfy them. The activities also form the basis for a deliverology schedule that accompanies the strategy as Appendix B.

- The IM Strategy was presented to, and endorsed by, the CSE IM/IT Steering Committee on 17 October 2016. IM/IT Committee October 17 Draft RoD: https://cerrid2.corp.cse/cerrid/llisapi.dll?func=ll&objaction=overview&objid=31795991

Next Steps

CIO will work closely with a communications representative to share strategy highlights and implications with staff.

Recommendation

It is recommended that the Chief approve the CSE *Enterprise IM Strategy 2017 and Beyond.*
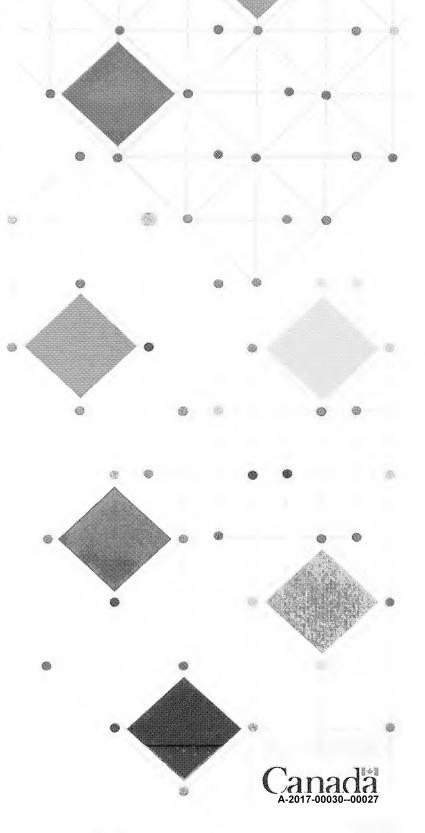
———

A/CIO
IMSO

Reviewed by:

Director, Information Management

Communications Security
Establishment

Centre de la sécurité
des télécommunications

DELIVERING THE INFORMATION ADVANTAGE

Enterprise Information Management Strategy
2017 and Beyond

Canada

"To manage a business well is to manage its future; and to manage the future is to manage information."

- Marion Harper Jr.

A-2017-00030--00028

INTRODUCTION

Information, along with people, finances and infrastructure, are key strategic resources in the Government of Canada and is at the very core of CSE's operations. Information is the foundation of everything we do, from service delivery and planning activities to decision-making and policy development.

The quality, reliability and integrity of information are critical to the fulfillment of our mandate, and can only be ensured through enterprise-wide information management (IM). CSE's IM Program supports the delivery of services across the organization for the protection and security of records throughout the lifecycle, while assisting in providing efficient systems for access to the information.

Because of the sensitivity of our information, it is essential that we have the highest IM standards in place. The vast accumulation of information and the added complexity of collaborative ecosystems across the intelligence community, nationally and internationally, create challenges for us. We face a fundamental choice between being in a constant state of catch-up, and opportunity; implicit in this concept is the idea that we are entering a period that requires a transformation in how we manage our information.

The objectives of this enterprise strategy are clear – acknowledge the value of CSE's information, the importance of managing CSE's information at an enterprise level, and the benefits of treating CSE's information as a strategic asset. Every employee is responsible for the success of this strategy – regardless of role, working level, or business line. As CSE employees, we are the stewards of the information we collect and create. It is our duty to safeguard this information as a public trust, and manage it as an asset to maximize its value in the service of Canadians.

WHERE WE ARE TODAY

We are well positioned...

CSE has a mature information management governance structure that provides leadership. This structure is clearly articulated in CSE's policy suite which explains the responsibilities, accountabilities, and expectations of CSE employees in carrying out IM activities. A culture of evidence-based decision making supports good governance by using monitoring and reporting processes as the primary reference for refining existing, and planning new, initiatives.

We have engaged Library and Archives Canada to issue a suite of Records Disposition Authorities that gives us the legal right to dispose of our information. To complement these instruments, we have worked with the business lines to develop records retention and disposition schedules that describe the types of information we have, how long we are required to keep this information, and how we are to dispose of it when the time comes.

Our move from the Confederation Heights Campus to the Edward Drake Building has forced us to reduce our paper footprint and adopt healthy practices to minimize office clutter. Paper reduction goals have also been met through the digitization of paper documents; in fact, CSE was one of the first departments in the Government of Canada to implement such a program.

For the past decade CSE has kept up with the latest Treasury Board-approved Enterprise Content Management (ECM) systems. CERRID ensures standardized electronic document and record management across all business lines. A robust training and awareness program that is dedicated to providing a customized service supports this system through a number of channels, including in-class training, computer-based modules and one-on-one sessions.

During the 2015-2016 Management Accountability Framework (MAF) assessment period, CSE was evaluated on IM and was commended by Treasury Board for its stewardship. CSE completed 100% of planned paper and electronic disposition activities, well above the Government of Canada average, and submitted its departmental Open Government Implementation Plan.

... But not without challenges

While CSE has invested in a designated corporate repository, CERRID, this system does not currently contain and manage all of the organization's unstructured electronic information. CSE stores its information in a number of formats and distributes them across multiple applications and platforms. This practice complicates the search and retrieval process. Moving our holdings into the designated corporate repository will not only help curb the negative effects of information overload, it will better support collaboration and evidence-based decision making.

We know that the volume of information we collect and create is growing at an exponential rate, but are we ready for it. We are creating 150,000 new documents monthly in CERRID alone. Moreover, a recent inventory of our IT infrastructure shows that we have an additional 112 data and information repositories that need to be managed. Although the price of digital storage is on the decline in the real world, CSE could invite additional costs for surpassing storage quotas under its private sector partner agreement. Keeping information longer than we should may also expose the organization to the unnecessary production of stale records in response to Access to Information and Privacy (ATIP) requests, as well as prolonged eDiscovery.

The biggest challenge to achieving the highest level of information management maturity is human. The key to success rests squarely on collaboration, coordination, and cooperation. Employees are also looking for more lightweight systems to perform their work – systems that mirror what they have in their personal lives. We need to strike a balance between traditional time tested practices and newer disciplines that allow information to be handled with more flexibility.

BUSINESS DRIVERS

Although progress has been made on how we manage information, we need to shift toward realizing and sustaining an information advantage for improved business outcomes. The following represents a sample of the business-driven IM requirements that need to be addressed and supported by this strategy.

Driver: Legislated Compliance

Departmental accountabilities, responsibilities and requirements have evolved following the Treasury Board refresh of the IM Policy Suite and Strategy for the Government of Canada, as well as changes to Library and Archives Canada's direction on documentary heritage. CSE will adapt to these changing requirements by ensuring it has the appropriate policies and processes in place.

Driver: Appropriate Collection and Use of Open Source Information Resources

In order to effectively leverage increasing quantities of publicly available information, CSE must assess its current open source information holdings, identify additional information requirements, and ensure appropriate governance of the acquisition, management and use of open source collections. The way in which open source products and services are produced, managed and delivered must undergo a significant transformation. There is a need for innovative, value-added open source products and services that focus on

s.15(1) - DEF

Driver: Diminished Information Risks

Complex organizations like CSE require increasingly sophisticated safeguards to prevent security and privacy breaches. The workforce must understand and apply proper IM practices for sharing and protecting information. It must also exercise its duty to document and its duty to delete. Working in tandem with information security, privacy, litigation and IT specialists, we can begin to develop and implement mitigation measures to reduce risks and improve the integrity of our information.

Driver: Knowledge Gap

The knowledge gap manifests itself on multiple levels, from the individual level all the way to the enterprise level. CSE is facing a wave of impending retirements of long-tenured experts. As each of these valuable resources departs the organization, we need to consider continuity. Moving toward a future where information is used to its fullest potential will require training to aid employees, including IM functional specialists, in acquiring skills for effective IM.

⚙ Driver: Data Analytics Imperative

CSE faces increasing demands from across the enterprise for data analytics solutions to address rapidly increasing data volumes. Data literacy will become a core skillset to be embedded throughout the enterprise. The need for data analytics permeates the mission with impacts on foreign intelligence analysis, business intelligence, global situational awareness, and corporate governance. The need to acquire, process, manage and use vast quantities of data, often in real time, will require investment in tools, training and infrastructure; the increased importance of open source data will also require that adequate low side infrastructure be in place in order to effectively extract value from that data.

⚙ Driver: Disruptive Business, Service and Technology Trends

Trends in IM present opportunities for change and innovation, and these must be seized. To stay relevant, CSE must reach out to key partners and devote time and money to experimenting with new approaches and technology trends for addressing growing IM challenges.

⚙ Driver: Digital Collaboration

To allow for genuine collaboration across the department and the S&I community, CSE needs to reduce information silos, integrate IM practices and automate business processes. CSE must find ways to facilitate knowledge sharing and re-uses of existing information resources. In transitioning to fully digital information collections, CSE must decrease its paper footprint and enable a collaborative environment in which information can be widely accessed. This will involve building and modernizing the Canadian Top Secret Network, and assessing opportunities for shared initiatives to strengthen cooperation and realize efficiencies. For initiatives with IM implications, CSE will have to determine how it manages responsibility for full compliance (i.e. ATIP, IM, records management and legal disclosure obligations being met).

A-2017-00030--00033

WHERE WE WANT TO BE

Our Vision is to foster an organizational culture where information is safeguarded and managed as a shared strategic asset to advance CSE's cyber mission.

We have identified four key areas of opportunity that will move CSE along the maturity curve from proactive to transformational IM. At the end of our journey, we will be able to declare that:

WE ARE MATURE:

CSE continues to excel at organizational recordkeeping, embraces the move towards greater openness and makes conscious changes in IM practices and investments to improve specific business outcomes.

WE ARE COMPLIANT:

CSE has strengthened policy and legislative compliance and holds the organization accountable for its IM practices.

WE ARE SERVICE-ORIENTED:

CSE offers best-in-class enterprise services to remain relevant from a service offering perspective and also aligned to the objectives of the business.
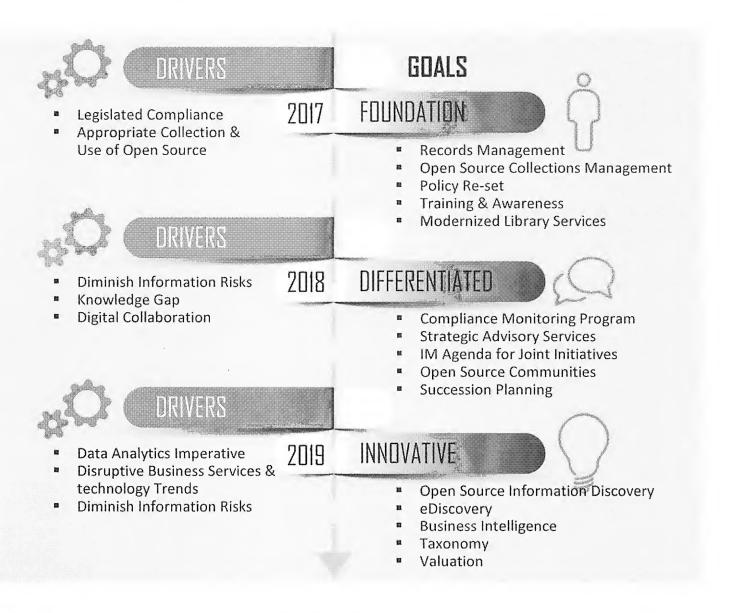
WE ARE LINKED:

CSE has engaged key partners to transform its capacity, shifting our philosophical outlook of IM and exploiting our information in imaginative ways.

A-2017-00030--00034

HOW WE WILL GET THERE

Each area of opportunity includes a number of strategic goals that serve to address business drivers and describe our desired future state. These goals are supported by key activities that identify the specific steps needed to satisfy them. The activities also form the basis for an implementation plan that accompanies this strategy.

The timeline below is a high level view of the strategy and how it supports our vision. Goals are categorized by level of complexity:
1. **Foundation** – meeting our essential IM requirements.
2. **Differentiated** – growing our capacity to become more agile with our information.
3. **Innovative** – piloting new ideas to transform our IM posture.

DRIVERS   **GOALS**

2017 — FOUNDATION

DRIVERS
- Legislated Compliance
- Appropriate Collection & Use of Open Source

Goals:
- Records Management
- Open Source Collections Management
- Policy Re-set
- Training & Awareness
- Modernized Library Services

2018 — DIFFERENTIATED

DRIVERS
- Diminish Information Risks
- Knowledge Gap
- Digital Collaboration

Goals:
- Compliance Monitoring Program
- Strategic Advisory Services
- IM Agenda for Joint Initiatives
- Open Source Communities
- Succession Planning

2019 — INNOVATIVE

DRIVERS
- Data Analytics Imperative
- Disruptive Business Services & technology Trends
- Diminish Information Risks

Goals:
- Open Source Information Discovery
- eDiscovery
- Business Intelligence
- Taxonomy
- Valuation

A-2017-00030--00035

STRATEGIC GOALS

OPPORTUNITY 1: Mature Records & Collections Management

Goal 1: Records Management
Goal 2: Open Source Collections Management

OPPORTUNITY 2: Compliance

Goal 3: Policy Reset
Goal 4: Compliance Monitoring Program
Goal 5: Training & Awareness

OPPORTUNITY 3: Best-In-Class Service Delivery

Goal 6: Strategic Advisory Services
Goal 7: Open Source Information Discovery (OSID)
Goal 8: Modern Library Services
Goal 9: eDiscovery
Goal 10: Business Intelligence

OPPORTUNITY 4: Innovation Through Partnership

Goal 11: IM Agenda for Joint Initiatives
Goal 12: Open Source Communities
Goal 13: Industry & Academia Touchpoints

Appendix A: Mapping to CSE Vision 2020 Strategic Direction

Appendix B: Implementation Plan

A-2017-00030--00036

OPPORTUNITY 1: Mature Records & Collections Management

WE ARE MATURE

Bringing CSE to a higher level of maturity where policy and legislative requirements are fully met and the department has access to high-quality, authoritative information to support its business goals.

1 : Records Management

Manage the physical and digital records of the department, identifying possible datasets for release through the Government of Canada's Open Government initiative and ensuring adherence to legislative, Treasury Board and Library and Archives Canada requirements for organizational recordkeeping.

KEY ACTIVITIES

- Create an inventory that identifies and contextualizes CSE's information repositories of business value.
- Maximize the release of information in support of the Government's Open Government initiative, subject to valid security and privacy exceptions.
- Identify key areas of risk to CSE's information resources and implement mitigation strategies.
- Increase disposition on structured data in corporate databases.
- Streamline processes for managing and transferring records of archival value.
- Continue digitization initiatives.

2 : Open Source Collections Management

Enhance traditional library services to better align with corporate and mission objectives and to optimize the department's open-source collections.

KEY ACTIVITIES

- Issue a collection development policy that sets out well-defined criteria for inclusion in CSE's open source collections.
- Acquire and sustainably manage commercial electronic resources that are targeted to the various CSE communities.
- Upgrade the library's cataloguing software to enable federated searching across the Tutte Institute for Mathematics and Computing (TIMC) and the corporate library collections.
- Enhance the user interface and promote the broader use of CSE's open source information resources.

A-2017-00030--00037

OPPORTUNITY 2: Compliance

WE ARE COMPLIANT

Strengthening policy and legislative compliance by implementing renewed policies, performing a monitoring and reporting function, and revamping the training program.

3 : Policy Reset

Create a cohesive IM policy suite to ensure consistency and proper alignment with CSE and Government of Canada direction.

KEY ACTIVITIES

- Review, update and consolidate IM policies.
- Address policy gaps e.g. Open Government obligations, process for departing employees, eDiscovery, Open Source Information Discovery activities, etc.

4 : Compliance Monitoring Program

Establish a compliance monitoring function in IM whereby information systems and settings would be actively monitored for policy compliance.

KEY ACTIVITIES

- Identify theme activities for assessing compliance with Treasury Board and departmental IM policies and follow-up actions for non-compliance.
- Establish governance for the program to include key accountabilities and responsibilities within CSE with respect to the monitoring process as well as reporting requirements.
- Conduct a pilot project involving a chosen business line.

5 : Training & Awareness

Strengthen employee understanding of their individual accountabilities, and drive awareness and change within the culture of the business lines.

KEY ACTIVITIES

- Develop and implement a mandatory IM awareness session for all CSE employees.
- Make better use of IM didactic material available across Government for internal re-use.

A-2017-00030--00038

OPPORTUNITY 3: Best-In-Class Service Delivery

Reaching new levels of excellence by growing and modernizing existing services and introducing new services.

⬚ 6 : Strategic Advisory Services

Provide insight and guidance at a strategic level to strengthen internal IM governance and promote CSE's role as a leading expert of Government of Canada IM solutions in the top secret environment.

KEY ACTIVITIES

- Continue conducting digital disposition activities on unstructured data and institutionalize best practices through policy, training & awareness and/or compliance monitoring.
- Enhance CSE's information architecture by ensuring tools, systems and technical solutions implement enterprise IM requirements.
- Pioneer the role of the Data Steward.

⬚ 7 : Open Source Information Discovery (OSID)

Expand the role of OSID to serve as an S&I community centre of excellence for the analysis, reporting and dissemination of products and services derived from OS information, and to effectively organize the acquisition and management of OS information, resources and tools.

KEY ACTIVITIES

- Assess and acquire a variety of OS tools and data sets.
-
- Develop innovative   products and service delivery options.
- Develop OSID tradecraft and techniques.
-

OPPORTUNITY 3: Best-In-Class Service Delivery

WE ARE SERVICE-ORIENTED

Reaching new levels of excellence by growing and modernizing existing services and introducing new services.

8 : Modern Library Services

Connect employees with the Open Source electronic and print information they need to be successful in their work through in-depth research, annotated bibliographies and a modern online presence.

KEY ACTIVITIES

- Implement enhanced processes and/or systems to better gather, track and analyze client requirements for open source research and material.
- Enhance research products by leveraging OSID tools and optimize dissemination platforms.

9 : eDiscovery

Introduce an in-house expertise capable of performing electronic searches across all information systems in support of access to information and litigation requests, which will allow the department to execute discovery consistently and increase the level of quality control.

KEY ACTIVITIES

- Codify the processes for identifying information that must be produced for access to information or litigation purposes.
- Implement a new capability to perform searches across the increasingly complex technology and application infrastructure at CSE.

10 : Business Intelligence (BI)

Develop a modern BI service by creating a holistic approach that leverages technical innovations, data analytics, and user engagement.

KEY ACTIVITIES

- Assess and document existing BI initiatives within CSE.
- Develop a strategic overview of emerging BI trends and standards.
- Explore a proper governance model, innovative analytic solutions, and integrated information management.

A-2017-00030--00040

s.15(1) - DEF

s.21(1)(b)

OPPORTUNITY 4: Innovation Through Partnership

WE ARE LINKED

Unlocking transformational change by engaging other government departments, 5-Eyes and private sector partners to leverage lessons learned, collaborate on initiatives and keep up-to-date on latest industry trends.

11 : IM Agenda for Joint Initiatives

Engage with CSIS in ongoing bilateral knowledge sharing and work collaboratively with Government of Canada departments that are involved in rolling out shared services to ensure desirable features can be leveraged by CSE as well as OGD's IM and records management programs.

KEY ACTIVITIES

- Continue working with CSIS under the auspices of Integrated Internal Services Working Groups.
- Explore a   for OS collections.
- Champion the adoption of   and partner with   on piloting configurations (e.g. Auto-classification, eDiscovery Rights).
- Participate in other centrally coordinated working groups to influence technical developments related to IM (e.g. MyGCHR).

12 : Open Source Communities

Actively develop a network of national and international partnerships in the Open Source information space.

KEY ACTIVITIES

- Nationally, stand up an active community of interest focused on sharing OS expertise and products by leveraging expertise of   . These partners will form the core of a working group.
- Internationally, take advantage of the International Open Source Working Group (IOSWG) to

A-2017-00030--00041

OPPORTUNITY 4: Innovation Through Partnership

WE ARE LINKED

Unlocking transformational change by engaging other government departments, 5-Eyes and private sector partners to leverage lessons learned, collaborate on initiatives and keep up-to-date on latest industry trends.

13 : Industry & Academia Touchpoints

Partner with industry and academia to keep abreast of the latest trends and thinking and help evolve CSE's IM practices.

KEY ACTIVITIES

- Explore approaches and tools for implementing a CSE taxonomy.
- Explore a sustainable and whole-of-system approach to the valuation of CSE information assets.
- Work with vendors on tools development.
- Develop an academic outreach program for IM/RM succession planning and strategic advancements.

Appendix A: Mapping to CSE Vision 2020 Strategic Direction

IM Strategic Goals	CSE Strategic Direction			
	Trust and Confidence	A Lead Authority in Cyber Security	Premier Services in Cyber Operations	Enterprise Service Provider for the S&I Community
Records Management	✓			
Open Source Collections Management		✓	✓	
Policy Reset	✓			✓
Compliance Monitoring Program	✓			✓
Training & Awareness	✓			✓
Strategic Advisory Services			✓	✓
Open Source Information Discovery (OSID)		✓	✓	
Modern Library Services		✓	✓	
eDiscovery	✓			
Business Intelligence	✓		✓	
IM Agenda for Joint Initiatives				✓
Open Source Communities		✓	✓	
Industry & Academia Touchpoints	✓			✓

A-2017-00030--00043

Appendix B-Ia: Implementation Plan
Mature Records & Collections Management - Records Management

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Create an inventory that identifies and contextualizes CSE's information of business value.	▪ CSE has an inventory that enables sound decision making, services, ongoing reporting and answers performance and accountability requirements.	▪ Increased use of the inventory across the organization.
▪ Maximize the release of information in support of the Government's Open Government initiative, subject to valid security and privacy exceptions.	▪ A drive for openness that is embedded in CSE culture and processes. ▪ CSE contributes to the Open Data Dialogue through the release of data sets and transfers of information resources of enduring value (IREV).	▪ Inventory of data and *information* resources of business value is complete and current. ▪ Public releases of CSE datasets and information resources on open.canada.ca increase yearly in accordance with TBS direction. ▪ CSE has maximized the removal of access restrictions on departmental IREV prior to transfer to LAC.
▪ Identify key areas of risk to CSE's information resources and implement mitigation strategies.	▪ Information that is essential to running our business is available in the face of physical or technological disaster. ▪ There is an established risk register for identifying risks to information resources and creating risk profiles specific to IRBVs. ▪ Personal information is retained and disposed of to meet *Privacy Act* and Access to Information and Privacy (ATIP) requirements. ▪ Appropriate use of system access permissions and classification.	▪ Essential records are identified and protected. ▪ Inappropriate or inadvertent information disclosures or loss incidents are minimized.
▪ Increase disposition on structured data in corporate databases.	▪ Increase in accountability to TBS and LAC on the disposition of corporate information. ▪ ATIP and litigation risks diminish.	▪ Automated disposition capabilities are included in new systems.
▪ Streamline processes for managing and transferring records of archival value.	▪ LAC policy requirements for documentary heritage are met. ▪ Records disposition authorities (RDAs) are current. ▪ CSE manages born-digital information.	▪ Declassification/downgrading program and/or policies are established. ▪ Current RDAs are updated and integrating into a single document. ▪ CSE has implemented a formal program to manage born-digital information.
▪ Continue digitization initiatives.	▪ Reduce our physical footprint and modernize processes. ▪ Increased searchability of information holdings.	▪ Physical space occupied decreases. ▪ Reduced search time for information retrieval.

A-2017-00030--00044

Appendix B-1b: Implementation Plan
Mature Records & Collections Management - Open Source Collections Management

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Issue a collection development policy that sets out well-defined criteria for inclusion in CSE's open source collections.	▪ CSE has an open source collection that precisely links to CSEs mandates.	▪ Loans as a percentage of the collection increase by 20%.
▪ Acquire and sustainably manage commercial electronic resources that are targeted to the various CSE communities.	▪ Funds are accountably spent and budget has flexibility embedded. The value for dollars for the collection is made apparent.	▪ Usage metrics for the commercial resources is monitored and all seats are in use.
▪ Upgrade the library's cataloguing software to enable federated searching across the TIMC and the corporate library collections.	▪ Both CSE library catalogues can be searched in one place.	▪ Number of library requests that originate in the catalogue increase by 15%.
▪ Enhance the user interface and promote the broader use of CSE's open source information resources.	▪ Information resources for the enterprise are easy to find, use and share.	▪ Every resource sees an increase in page views.

Appendix B-2: Implementation Plan

Compliance – Policy Reset

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Review, update and consolidate IM policies.	▪ Consistent management of CSE information.	▪ Targeted IM behaviour improves by 10%.
▪ Address policy gaps e.g. Open Government obligations, process for departing employees, eDiscovery, Open Source Information Discovery activities, etc.	▪ All IM requirements are covered by policy.	▪ Annual policy gap analysis shows diminished gaps from previous year.

Compliance – Compliance Monitoring Program

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Identify theme activities for assessing compliance with Treasury Board and departmental IM policies and follow-up actions for non-compliance.	▪ Compliance plan that identifies theme activities.	▪ Plan complete and in place by target date. ▪ With plan complete, able to move to the next step, governance.
▪ Establish governance for the program to include key accountabilities and responsibilities within CSE with respect to the auditing and monitoring processes as well as reporting requirements.	▪ Governance model is in place.	▪ Policy instrument issued and promulgated to support IM monitoring and reporting.
▪ Conduct a pilot project with a chosen business line.	▪ A business line is subject to monitoring of one theme activity for a six month period.	▪ Reporting results in behavioural change.

Compliance – Training & Awareness

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Develop and implement a mandatory IM awareness session for all CSE employees.	▪ Employees are informed of their IM responsibilities.	▪ Percentage of employees trained achieves and stays over 90%.
▪ Make better use of IM didactic material available across Government for internal re-use.	▪ CSE spends less time creating material and reuses what is available from OGDs.	▪ Percentage of new versus reused material. Reused material exceeds 50%.

A-2017-00030--00046

Appendix B-3a: Implementation Plan

Best-In-Class Service Delivery – Strategic Advisory Services

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Continue conducting digital disposition activities on unstructured data and institutionalize best practices through policy, training & awareness and/or compliance monitoring.	▪ CSE employees perform their information lifecycle duties delegated to them from the *Policy on Information Management*.	▪ Increase of finalized documents within the corporate repository.
▪ Enhance CSE's information architecture by ensuring tools, systems and technical solutions implement enterprise IM requirements.	▪ Information management is integrated into tools, systems and technical solutions. ▪ Principles of reuse and information authority are adhered to.	▪ All new business requirements documentation includes information management requirements as identified by TBS for the IRBV inventory.
▪ Pioneer the role of the Data Steward.	▪ Improved IM across the organization. ▪ Data Stewards deliver tailored service to meet specific client needs.	▪ Reduction in HPSM tickets requesting IM assistance.

Best-In-Class Service Delivery – Open Source Information Discovery (OSID)

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Assess and acquire a variety of OS tools and data sets.	▪ An inventory of robust analytic tools and a wide range of open source information resources are in place.	▪ Tools are assessed against a set of established performance criteria. ▪ At least two analytic tools are procured and in use by target date.
▪ Develop innovative products and service delivery options.	▪ Reporting available in multiple formats across different platforms.	▪ Three kinds of reporting templates in active use: Ongoing Topic Briefs, and Deep Dive Research Papers. ▪ Products available via an OSID dedicated portal and at least one other delivery method. Some products
▪ Develop OSID tradecraft and techniques.	▪ OSID team is a center of analytic excellence for open source information acquisition, collation, synthesis, analysis and dissemination tradecraft.	▪ An OSID Analyst's Handbook is produced and kept up to date with analytic tradecraft, training tips and best practices.

A-2017-00030--00047

Appendix B-3b: Implementation Plan

Best-In-Class Service Delivery – Modern Library Services

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Implement enhanced processes and/or systems to better gather, track and analyze client requirements for open source research and material.	▪ The library is familiar with their clients and monitors all requests. ▪ Management is made aware of the requests being completed.	▪ Monthly metric reports on client requests completed.
▪ Enhance research products by leveraging OSID tools and optimize dissemination platforms.	▪ The library's products are improved, promoted and at the fingertips of analysts.	▪ Products viewed 20% more.

Best-In-Class Service Delivery – eDiscovery

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Codify the processes for identifying information that must be produced for access to information or litigation purposes.	▪ Appropriate information is produced with consistency, security and confidentiality.	▪ Reduced resources and time spent in eDiscovery. ▪ CSE processes are consistent and auditable.
▪ Implement a new capability to perform searches across the increasingly complex technology and application infrastructure at CSE.	▪ Legally defensible and auditable controls are in place.	▪ Legal hold capability exists across the enterprise. ▪ Ability to collect forensics evidence and demonstrate compliance.

Best-In-Class Service Delivery – Business Intelligence

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Assess and document existing BI initiatives within CSE.	▪ A broad understanding of BI activities across the enterprise.	▪ A consolidated report detailing all current and currently proposed BI initiatives is produced.
▪ Develop a strategic overview of emerging BI trends and standards.	▪ Ability to assess the level of BI maturity across CSE.	▪ A report on BI standards is produced, complete with recommendations for implementation.
▪ Explore a proper governance model, innovative analytic solutions, and integrated information management.	▪ Foundational strategy in place for the implementation of enterprise-wide BI.	▪ A comprehensive BI strategy prepared and presented to IM/IT SC.

Appendix B-4a: Implementation Plan
Innovation Through Partnership – IM Agenda for Joint Initiatives

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Continue working with CSIS under the auspices of Integrated Internal Services Working Groups.	▪ Opportunities are assessed and implemented to strengthen cooperation, collaboration and realize efficiencies.	▪ A detailed analysis (i.e. value proposition, impact and implementation) and recommendations on IM-related potential shared service initiatives, such as RM, data management, archival services, library services, etc. is completed.
▪ Explore a for OS collections.	▪ CSE and CSIS have a joint vision for OS collections.	▪ An options analysis for the of OS collections is complete and a decision reached.
▪ Champion the adoption of and partner with on piloting configurations (e.g. Auto-classification, eDiscovery Rights).	▪ A strong partnership with aligns our platforms for a common approach.	▪ Evaluation of capabilities. ▪ Quarterly meetings with on specific agenda items.
▪ Participate in other centrally coordinated working groups to influence technical developments related to IM (e.g. MyGCHR).	▪ IM Requirements are built into new applications.	▪ Regular meetings with relevant stakeholders.

Innovation Through Partnership – Open Source Communities

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Nationally, stand up an active community of interest focused on sharing OS expertise and products by leveraging expertise of These partners will form the core of a working group.	▪ Closer collaboration between agencies.	▪ The COI meets at least twice a year.
▪ Internationally, take advantage of the International Open Source Working Group (IOSWG) to	▪ Analytic knowledge transfer and increased CSE capabilities.	▪ Increased contributions of CSE products to ▪ Team members make presentations to both IOSWG events every year. ▪ An international integree is embedded within the OSID team for at least six months.

Appendix B-4b: Implementation Plan
Innovation Through Partnership – Industry & Academia Touchpoints

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Explore approaches and tools for implementing a CSE taxonomy.	▪ Recommendation on a CSE taxonomy.	▪ Development of white paper is monitored.
▪ Explore a sustainable and whole-of-system approach to the valuation of CSE information assets.	▪ A valuation approach that allows CSE to categorize its information assets, potentially reduce inventory carry costs, and help prioritize and budget IT/business initiatives.	▪ A proposed method of measuring information quality and value characteristics. ▪ A process for performing, reviewing, and communicating information asset valuation assessments.
▪ Work with vendors on tools development.	▪ Vendors have implemented desired features.	▪ The team identifies at least two opportunities for tool development, such as improved auditing function in analytic tools, and works directly with the vendor to enhance capabilities.
▪ Develop an academic outreach program for IM/RM succession planning and strategic advancements.	▪ IM succession planning and strategic advancements is improved.	▪ Biannual meetings with academic partners.

Recommended by:

Date:

Director, Information Management (CIO-E)

Endorsed by:

Date:

Acting Deputy Chief - Chief Information Officer (CIO)
Information Management Senior Official (IMSO)

Approved by:

Date: FEB 0 6 2017

Greta Bossenmaier
Chief, Communications Security Establishment

<u>CSE – CSIS Update to the National Security Advisor</u>
(For Approval)

Summary

- Attached for your signature is a letter to the National Security Advisor, developed jointly by CSE and CSIS, to provide an update on the ongoing collaborative work between our two agencies.

- The letter has been approved at the ADM level at both agencies.

- Upon your signature, the letter will be provided to Director Coulombe for signature and then provided to the NSA.

Dominic Rochon
Deputy Chief, Policy and Communications

CCM #: 25675 CERRID #: 31292832

MEMORANDUM TO THE NATIONAL SECURITY ADVISOR

CSE-CSIS COLLABORATION

ISSUE:

To provide an overview of current priority areas of collaboration between the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE).

BACKGROUND:

CSIS and CSE have common national security goals and share a number of challenges in keeping Canada, Canadians and Canadian interests safe and secure. The two agencies continue to work collaboratively in accordance with our respective mandates and legislative authorities to effectively fulfill the government's national security intelligence requirements.

The CSE-CSIS Joint Management Team (JMT) – a group comprised of members of both Executive Committees – is the agencies' senior forum for setting priority activities for cooperation and addressing issues of mutual interest. The JMT is supported by four ADM-level sub-groups that meet as required, specifically the Operational, Cyber, Corporate, and Integrated Internal Services JMT Pillars.

AREAS OF COLLABORATION:

Operational Pillar

CSIS and CSE have recently set strategic directions to lead them through the next five years, and are well aligned to with common priorities in   and shared services. Over recent months, CSE has

The passage of Bills C-44 and C-51 has required an evolution of the agencies' policy instruments and work continues on the implementation of these changes. Bill C-44 has allowed CSE to support CSIS more effectively in the pursuit of Canadian targets, predominantly outside Canada. At present, CSE is providing assistance on

Bill C-51 has opened a new area of collaboration between the agencies – threat reduction – and a Memorandum of Understanding was signed in June 2016 to guide this collaboration.

s.15(1) - DEF

s.16(1)(b)

s.16(1)(c)

s.21(1)(b)

The agencies continue to mature collaboration

CSE and CSIS have been working together on advancing relations with designated partners

In addition to the above, there are other established areas of collaboration and personnel exchange. For example,

Collaborative work is underway to   to reduce the likelihood of duplication.

Other areas of collaboration include   In addition, through standing requests for assistance, CSIS takes advantage of CSE's technical capabilities

Cyber Pillar

The agencies created a distinct Pillar for cyber to reflect the importance placed on cyber issues and ensure they are addressed on a regular basis.

The agencies have also developed a governance structure

s.15(1) - DEF
s.16(1)(c)
s.21(1)(b)
s.69(1)(g) re (a)
s.69(1)(g) re (f)

Moving forward, CSIS and CSE will prioritize cyber engagement

We are also enhancing collaboration in the

Corporate Pillar

Corporate collaboration between CSIS and CSE spans the policy, communications, finance, human resources,
and these counterparts meet regularly. Domestically, we collaborated closely

The agencies are also currently

Moving forward, we plan to coordinate on how to best support the National Security and Intelligence Committee of Parliamentarians, and to implement any policy, legal, or operational changes required as a result of possible amendments to Bill C-51.

Internationally, the agencies coordinated on travel to Five Eyes countries, namely to attend and deliver joint remarks at the   meeting that took place
                    and to meet with our   partners   to discuss multi-agency collaboration. Recently, we also jointly hosted a   CIO forum which proved to be very successful.

Being co-located continues to benefit the agencies' relationship-building and cultural awareness efforts. We frequently extend invitations for events and host joint CSE-CSIS gatherings such as GCWCC events and an annual CSE-CSIS volleyball tournament. Our proximity also encourages collaboration on internal communications, for example our recent communication
       and we liaise on public communications such as our respective Twitter accounts.

Integrated Internal Services Pillar

Integrated Internal Services (IIS) is an initiative that was launched in March 2016 that will allow CSE and CSIS to become more resilient within a joint community by leveraging best practices for internal services and building on each other's strengths. Co-location has seen areas for collaboration naturally arise,   to official languages,
       Further, the agencies have begun 12-month pilots in the   materiel management, and finance domains, during which a small number of participating employees are moving from one organization to the other, providing services to both.

A second wave of pilots to begin this year will cover further areas within   finance, as well as areas in procurement, emergency management, and communications. One specific example of

3

an IIS initiative is the plan to shift to a single Enterprise Resource Planning System to support financial and Asset management at both agencies, which will replace some of our   financial, procurement and asset management legacy applications.

We trust that you will find this overview of our collaboration to be a helpful contribution. As always, please do not hesitate to contact us should you require further information.

Greta Bossenmaier   Michel Coulombe
Chief, CSE   Director, CSIS

4